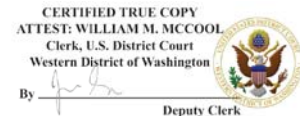


UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)
 Nine Gmail Accounts,
 more fully described in Attachment A

Case No. MJ20-713

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, incorporated herein by reference.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. §§ 2261A(2)(A), (B) Cyberstalking
 18 U.S.C. § 875(c) Interstate Threats

The application is based on these facts:

- ☒ See Affidavit of FBI Special Agent Matthew Zito, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

[Signature]
Applicant's signature

Special Agent Matthew Zito, FBI

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 11/05/2020

[Signature]
Judge's signature

City and state: Seattle, Washington

Hon. John L. Weinberg, United States Magistrate Judge

Printed name and title

AFFIDAVIT OF SPECIAL AGENT MATTHEW ZITO

STATE OF WASHINGTON)
)
) SS
COUNTY OF KING)

I, Matthew A. Zito, having been duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since 2012. I am currently assigned to the Seattle Safe Streets Task Force ("SSTF")/High Intensity Drug Trafficking Area ("HIDTA") Task Force. The SSTF/HIDTA squad is a task force comprised of FBI agents and SPD officers assigned to investigate the criminal activities of large-scale narcotics trafficking organizations, criminal street gangs, and incidents of violent crime. Prior to my assignment with the Seattle SSTF/HIDTA, I was assigned to the Los Angeles FBI, Los Angeles Strike Force ("LASF"), a task force comprised of agents and officers from federal, state, and local agencies assigned to investigate large-scale narcotics trafficking organizations. I have also previously been assigned to the Las Vegas division of the FBI, where I was assigned to a HIDTA Task Force investigating the drug trafficking activities of organized crimes groups associated with Mexican cartels.

2. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. I have personally participated in the execution of search warrants involving the search and seizure of computer equipment.

3. I make this affidavit in support of an application for a search warrant for information associated with certain Gmail account[s] that is stored at premises controlled by Google LLC, an email provider headquartered at 1600 Amphitheatre Parkway in Mountain

1 View, California. The Gmail accounts, referred to collectively as the SUBJECT
2 ACCOUNTS, are:

- 3 a. joshuasbusinessemail@gmail.com
- 4 b. joshistopforever@gmail.com
- 5 c. financingpsychology@gmail.com
- 6 d. joshua.thomas.seattle@gmail.com
- 7 e. proudtobeunamerican@gmail.com
- 8 f. contactjoshuabales@gmail.com
- 9 g. mastersshakejb@gmail.com
- 10 h. summerofgeorge1@gmail.com
- 11 i. joshuabcontact@gmail.com
- 12
- 13
- 14

15 4. The information to be searched is described in the following paragraphs and in
16 Attachment A. This affidavit is made in support of an application for a search warrant under
17 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC to disclose to
18 the government copies of the information (including the content of communications) further
19 described in Section I of Attachment B. Upon receipt of the information described in
20 Section I of Attachment B, government-authorized persons will review that information to
21 locate the items described in Section II of Attachment B.

22 5. As set forth below, I have probable cause to believe that the SUBJECT
23 ACCOUNTS to be searched will contain evidence of violations of Title 18, United States
24 Code, Sections 2261A(2)(A), (B) (Cyberstalking); and Title 18, United States Code, Section
25 875(c) (Interstate Threats), committed by Joshua Bales.

26 6. The facts set forth in this Affidavit are based on my own personal knowledge;
27 knowledge obtained from other individuals during my participation in this investigation,
28 including other law enforcement personnel; review of documents and records related to this

1 investigation; communications with others who have personal knowledge of the events and
 2 circumstances described herein; and information gained through my training and experience.
 3 Because this Affidavit is submitted for the limited purpose of establishing probable cause in
 4 support of the application for a search warrant, it does not set forth each and every fact that I
 5 or others have learned during the course of this investigation.

6 **JURISDICTION**

7 7. This Court has jurisdiction to issue the requested warrant because it is “a court
 8 of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A),
 9 & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has
 10 jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

11 **SUMMARY OF PROBABLE CAUSE**

12 **A. Investigative Background**

13 8. In October 2019, the Federal Bureau of Investigation (“FBI”) initiated an
 14 investigation into JOSHUA THOMAS BALES based on information received by a woman,
 15 referred to herein as X.C., who reported that, since 2017, BALES had been engaged in a
 16 course of conduct that placed X.C. in reasonable fear of death and serious bodily injury to
 17 X.C. and her family, and caused substantial emotional distress to X.C., as set forth in greater
 18 detail below.

19 9. Specifically, X.C. reported that between 2013 and 2017, BALES and X.C. were
 20 in a dating relationship. X.C. ended their dating relationship in 2017.

21 10. After their relationship ended in 2017, and at all times material to this
 22 investigation, BALES resided in the Western District of Washington, and X.C. resided in
 23 Australia.

24 11. X.C. reported that, since the end of their dating relationship, X.C. received
 25 hundreds of threatening email communications sent by BALES, as himself and
 26 anonymously, from various email addresses operated by Google, Inc.¹ The emails were
 27

28 ¹ Google, Inc., based in Mountain View, California, is an electronic communication service provider that provides email, file storage, and other electronic communications and storage services to users all over the world.

1 usually sent to X.C.'s personal email address: "[REDACTED]@gmail.com", and sometimes
2 to her university email address: "[REDACTED]@uni.sydney.edu.au." BALES controlled and
3 used email addresses that included "joshuasbusinessemail@gmail.com,"
4 "joshistopforever@gmail.com," "financingpsychology@gmail.com,"
5 "joshua.thomas.seattle@gmail.com," "proudtobeunamerican@gmail.com,"
6 "contactjoshuabales@gmail.com," "mastersshakejb@gmail.com,"
7 "summerofgeorge1@gmail.com," and "joshuabcontact@gmail.com."

8 12. The emails that BALES sent to X.C. contained harassing and threatening
9 statements, including, but not limited to, the following:

10 13. On or about September 13, 2018, using the account
11 "joshuasbusinessemail@gmail.com," BALES sent X.C. an email stating: "I will destroy your
12 life forever, I promise. Forever, until I kill you. You haven't seen anything yet. I haven't
13 even started yet. It's gonna get much bigger."

14 14. On or about September 26, 2018, using the account
15 "proudtobeunamerican@gmail.com," BALES sent X.C. an email stating: "I'm going to
16 Sydney and Adelaide to hunt you down. I'm gonna chop you up into little pieces and eat the
17 pieces and drink your blood."

18 15. On or about October 10, 2018, using the account
19 "joshistopforever@gmail.com," BALES sent X.C. an email stating: "I'm going to start
20 posting your nude pics in Muslim online forums for Sydney and Adelaide, with all your
21 details like both of your addresses and where you go to school. Why should I kill you, when
22 I can let them rape and kill you FOR me?"

23 16. On or about October 15, 2018, using the account
24 "financingpsychology@gmail.com," BALES sent X.C. an email with the subject line: "I
25 have to murder you." The email stated, "i WISH I was just joking, or that I could not kill
26 you. But...I have to. I have to kill you."

1 17. On or about October 25, 2018, using the account
2 “joshua.thomas.seattle@gmail.com,” BALES sent X.C. an email stating: “i’m going to kill
3 you and your whole family.”

4 18. On or about December 8, 2018, using the account
5 “joshua.thomas.seattle@gmail.com,” BALES sent X.C. an email with the subject line:
6 “homicide.” The email stated: “I am going to murder you. I swear it.”

7 19. On or about May 24, 2019, using the account
8 “contactjoshuabales@gmail.com,” BALES sent X.C. an email stating: “I’m going to kill
9 you.”

10 20. On or about May 31, 2019, using the account “mastersshakejb@gmail.com,”
11 BALES sent X.C. an email stating: “I loved you but you burned me. I’m going to throw acid
12 on your face.”

13 21. On or about July 13, 2019, using the account
14 “joshua.thomas.seattle@gmail.com,” BALES sent X.C. an email stating: “i’m gonna shoot
15 you with a compound bow and arrow, dead. i can buy compound bow and arrows legally in
16 Australia, very easily. With a compound bow and arrows, i could kill you and your whole
17 family very easily and very quickly: a matter of seconds only.”

18 22. On or about August 7, 2019, using the account
19 “summerofgeorgel@gmail.com,” BALES sent X.C. an email stating: “I swear to god I will
20 end your life. Sooner or later I will come to Australia and HUNT you down like an animal
21 and finish you!”

22 23. On or about September 7, 2019, using the United States Postal Service,
23 BALES mailed a letter from Seattle, Washington, to X.C.’s parents in Australia. In the
24 letter, BALES claimed to have naked photos and sex videos of X.C. Among other
25 defamatory statements contained in the letter, BALES characterized X.C. as “an animal, a
26 prostitute, a whore,” “a liar,” and “a snake,” and made disparaging allegations about X.C.’s
27 relationship with her parents.
28

24. On or about November 24, 2019, BALES, using the social media website Instagram², created a profile of X.C., without her consent, that featured her name and nude photographs of her. The profile description stated, "I'm a stupid, cheap, poor idiot who sucks dick for money to pay for Uni and homework. Contact me for more newd pics and sex vids."

25. On or about November 25, 2019, using the account "joshua.thomas.seattle@gmail.com," BALES sent X.C. an email stating: "i'm gonna do it again and again, [X.C.], make more accounts and do it again. And i'm gonna do worse; i'm gonna send your dad some things."

26. On or about November 25, 2019, using the account "joshua.thomas.seattle@gmail.com," JOSHUA THOMAS BALES sent X.C. an email stating: "that's what happens to TRAITORS! next time i'll contact even MORE of your contacts/followers/connections. Send me back my jacket and knife, along with an apology letter apologizing for being garbage and a traitor, or this will never end."

27. X.C. reported that BALES' numerous messages and course of conduct made her afraid that BALES would kill or seriously injure her and her family, and caused her substantial emotional distress. In an effort to avoid further unwanted contact with BALES, X.C. deactivated her social media accounts.

28. On or about December 3, 2019, investigators located and interviewed BALES. The interview was conducted in a public area of the University Village Mall, Seattle, Washington. During the interview, BALES was advised that the interview concerned threatening email communications BALES had been sending to X.C. BALES said that he understood why the interviewing agents wanted to speak with him. BALES said that he had

² Instagram, owned and operated by Facebook, Inc., based in Menlo Park, California, provides an interactive computer service and electronic communication service accessible to users all over the world through mobile phones and electronic devices using the Internet. Users of the service established Instagram accounts and chose unique usernames to associate with their accounts. Instagram allowed its users to create profile pages, post photos, post comments on other users' photos, and send direct messages to other Instagram users.

1 a very traumatic breakup with X.C. which caused him to do things he should not have done.
 2 He said that he was sorry for his behavior and it would stop immediately.

3 29. BALES admitted to creating an Instagram profile featuring nude photographs
 4 of X.C. BALES said that he added two friends of X.C.'s who he knew would alert her to the
 5 existence of the account but who were not likely share to the account with others. BALES
 6 said that he deliberately chose the least revealing photographs of X.C. in his possession
 7 because he just wanted to get her attention.

8 30. BALES was shown examples of emails sent to X.C. BALES admitted to
 9 controlling the email accounts and sending the emails to X.C. BALES was not detained at
 10 the conclusion of the interview. BALES said repeatedly throughout the interview that he
 11 would have no future communications with X.C.

12 31. On January 9, 2020, Google, Inc. provided subscriber information for the
 13 following email accounts. For each account, the subscriber name was some variation of
 14 BALES' name or initials:

Email Address	Subscriber Name
joshuasbusinessemail@gmail.com	Joshua Bales
joshistopforever@gmail.com	Josh B
financingpsychology@gmail.com	Josh Bales
joshua.thomas.seattle@gmail.com	Joshua Bales
proudtobeunamerican@gmail.com	Josh B
contactjoshuabales@gmail.com	Joshua Bales
mastersshakejb@gmail.com	mastersshakejb
summerofgeorge1@gmail.com	Joshua LastName

22 32. On or about Tuesday, March 10, 2020, X.C. reactivated her account with
 23 Instagram.

24 33. On or about Tuesday, March 10, 2020, using the account
 25 "joshuabcontact@gmail.com," BALES sent X.C. an email with the subject line: "Deactivate
 26 your Instagram account." The email stated: "I don't want another accident happening...do
 27 you?"
 28

1 34. On or about Tuesday, May 19, 2020, using the account
2 “joshua.thomas.seattle@gmail.com,” BALES sent X.C. an email with the subject line:
3 “Memories.” The email stated: “When you left, you said that I should try to let you keep
4 good memories of me/protect your memories of me in a good way. I dont [sic] care what
5 your memories of me are. But you should know that my memories of you are bad, memories
6 like you telling me “go die” on the phone whenever I was feeling down or alone. Also, delete
7 your Instagram account; I’m serious.”

8 35. On or about Tuesday, June 2, 2020, using the account
9 “mastersshakejb@gmail.com,” BALES sent X.C. an email stating: “I would have done
10 anything for you and been loyal forever, but now we are enemies forever instead. I still have
11 your underwear from when I took your virginity, and a LOT more things I can use against
12 you later ;).”

13 36. On or about June 3, 2020, using the account “summerofgeorge1@gmail.com,”
14 BALES sent X.C. an email stating: “I would have done anything for you; I would have been
15 loyal to you forever; I would have loved you forever. But the way you left, turned me into
16 your enemy forever. I still have your underwear, from when I took your virginity, and SO
17 much more that I will use against you in the future. Delete your Instagram account, unless
18 you want your naked photos and videos to become famous?”

19 37. On or about Sunday, June 14, 2020, X.C. reported that she discovered a new
20 Instagram account had been created with the display name “[X.C.]isgarbage.” The account
21 had a profile picture of a pair of women’s underwear, with text overlayed on the photograph
22 that said, “[X.C.] lost her virginity in these underwear.” The profile details include X.C.’s
23 name and the name “Josh B.”

24 38. On or about Monday, June 15, 2020, using the account
25 “contactjoshuabales@gmail.com,” BALES sent X.C. an email with the subject line, “delete
26 your instagram, or i will contact everyone about you.” The email stated: “delete your
27 instagram, or i will contact everyone about you. All your friends. Last time i only contacted a
28 couple friends.....this time i will contact EVERYONE, and will show them everything.”

BACKGROUND CONCERNING EMAIL

39. In my training and experience, I have learned that Google LLC provides a variety of on-line services, including electronic mail (“email”) access, to the public. Google LLC allows subscribers to obtain email accounts at the domain name Gmail.com, like the SUBJECT ACCOUNTS listed in Attachment A. Subscribers obtain an account by registering with Google LLC. During the registration process, Google LLC asks subscribers to provide basic personal information. Therefore, the computers of Google LLC are likely to contain stored electronic communications (including retrieved and unretrieved email for Gmail subscribers) and information concerning subscribers and their use of Gmail services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

40. In general, an email that is sent from a Gmail subscriber is stored in the subscriber’s “mail box” on Google LLC’s servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google LLC’s servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google LLC’s servers for a certain period of time.

41. A Gmail subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google LLC. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

42. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers,

1 means and source of payment (including any credit or bank account number). In my training
2 and experience, such information may constitute evidence of the crimes under investigation
3 because the information can be used to identify the account's user or users. Based on my
4 training and my experience, I know that, even if subscribers insert false information to
5 conceal their identity, this information often provides clues to their identity, location, or
6 illicit activities.

7 43. In my training and experience, email providers typically retain certain
8 transactional information about the creation and use of each account on their systems. This
9 information can include the date on which the account was created, the length of service,
10 records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of
11 the account (including whether the account is inactive or closed), the methods used to
12 connect to the account (such as logging into the account via the provider's website), and
13 other log files that reflect usage of the account. In addition, email providers often have
14 records of the Internet Protocol address ("IP address") used to register the account and the IP
15 addresses associated with particular logins to the account. Because every device that
16 connects to the Internet must use an IP address, IP address information can help to identify
17 which computers or other devices were used to access the email account.

18 44. In my training and experience, in some cases, email account users will
19 communicate directly with an email service provider about issues relating to the account,
20 such as technical problems, billing inquiries, or complaints from other users. Email
21 providers typically retain records about such communications, including records of contacts
22 between the user and the provider's support services, as well as records of any actions taken
23 by the provider or user as a result of the communications. In my training and experience,
24 such information may constitute evidence of the crimes under investigation because the
25 information can be used to identify the account's user or users.

26 45. As explained herein, information stored in connection with an email account
27 may provide crucial evidence of the "who, what, why, when, where, and how" of the
28 criminal conduct under investigation, thus enabling the United States to establish and prove

1 each element or alternatively, to exclude the innocent from further suspicion. In my training
2 and experience, the information stored in connection with an email account can indicate who
3 has used or controlled the account. This “user attribution” evidence is analogous to the
4 search for “indicia of occupancy” while executing a search warrant at a residence. For
5 example, email communications, contacts lists, and images sent (and the data associated with
6 the foregoing, such as date and time) may indicate who used or controlled the account at a
7 relevant time. Further, information maintained by the email provider can show how and
8 when the account was accessed or used. For example, as described below, email providers
9 typically log the Internet Protocol (IP) addresses from which users access the email account,
10 along with the time and date of that access. By determining the physical location associated
11 with the logged IP addresses, investigators can understand the chronological and geographic
12 context of the email account access and use relating to the crime under investigation. This
13 geographic and timeline information may tend to either inculcate or exculpate the account
14 owner. Additionally, information stored at the user’s account may further indicate the
15 geographic location of the account user at a particular time (*e.g.*, location information
16 integrated into an image or video sent via email). Last, stored electronic data may provide
17 relevant insight into the email account owner’s state of mind as it relates to the offense under
18 investigation. For example, information in the email account may indicate the owner’s
19 motive and intent to commit a crime (*e.g.*, communications relating to the crime), or
20 consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law
21 enforcement).

22 CONCLUSION

23 46. Based upon the information that has been uncovered during the course of this
24 investigation, and on the advice, experience, knowledge of other agents and officers involved
25 in this investigation, I believe these facts establish probable cause to search the SUBJECT
26 ACCOUNTS identified in Attachment A for the items described in Attachment B.

27 47. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is
28 not required for the service or execution of this warrant. The government will execute this

1 warrant by serving the warrant on Google LLC. Because the warrant will be served on
2 Google LLC, who will then compile the requested records at a time convenient to it,
3 reasonable cause exists to permit the execution of the requested warrant at any time in the
4 day or night.



MATTHEW ZITO, Affiant
Special Agent
Federal Bureau of Investigation

10 The above-named agent provided a sworn statement attesting to the truth of the
11 foregoing affidavit on the 5th day of November, 2020.



HON. JOHN L. WEINBERG
United States Magistrate Judge

ATTACHMENT A

(Accounts to be Searched)

This warrant applies to information associated with the following email addresses (SUBJECT ACCOUNTS) that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway in Mountain View, California.

The SUBJECT ACCOUNTS, are:

joshuasbusinessemail@gmail.com

joshistopforever@gmail.com

financingpsychology@gmail.com

joshua.thomas.seattle@gmail.com

proudtobeunamerican@gmail.com

contactjoshuabales@gmail.com

mastersshakejb@gmail.com

summerofgeorge1@gmail.com

joshuabcontact@gmail.com

ATTACHMENT B**Particular Items to be Seized****I. Information to be disclosed by Google LLC (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on November 2, 2020, the Provider is required to disclose the following information to the government for each SUBJECT ACCOUNT listed in Attachment A:

a. The contents of all emails associated with the account from January 1, 2018 to June 24, 2020, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken. The Provider is hereby ordered to disclose the above information to the government within 14 of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and instrumentalities of violations of Title 18, United States Code, Sections 2261A(2)(A), (B) (Cyberstalking); and Title 18, United States Code, Section 875(c) (Interstate Threats), those violations involving Joshua Bales and occurring after January 1, 2018, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Emails to and from the following email addresses:

a. [REDACTED]@gmail.com

b. [REDACTED]@uni.sydney.edu.au

(b) Photographs of X.C. or her personal items, such as underwear;

(c) Emails to X.C.'s family members, friends, and associates about X.C.;

(d) Emails about the sale or dissemination of information about X.C. or photographs of X.C.;

(e) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(f) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation; and

1 (g) The identity of the person(s) who created or used the email account, including records
2 that help reveal the whereabouts of such person(s).

3 This warrant authorizes a review of electronically stored information, communications, other
4 records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and
5 instrumentalities described in this warrant. The review of this electronic data may be conducted by
6 any government personnel assisting in the investigation, who may include, in addition to law
7 enforcement officers and agents, attorneys for the government, attorney support staff, and technical
8 experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic
9 data to the custody and control of attorneys for the government and their support staff for their
10 independent review.
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE
902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC, and my title is _____ . I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google LLC. The attached records consist of _____

[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)].

I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google LLC, and they were made by Google LLC as a regular practice; and

b. such records were generated by Google LLC's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature

UNITED STATES DISTRICT COURT

for the
Western District of WashingtonCERTIFIED TRUE COPY
ATTENT: WILLIAM M. MCCOOL
Clerk, U.S. District Court
Western District of WashingtonBy  Deputy ClerkIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
Nine Gmail accounts
more fully described in Attachment A)
)
)
)
)
)
)

Case No. MJ20-713

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Northern District of California
(identify the person or describe the property to be searched and give its location):

See Attachment A, attached hereto and incorporated by reference herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B, attached hereto and incorporated by reference herein.

YOU ARE COMMANDED to execute this warrant on or before November 19, 2020 (not to exceed 14 days)☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to any U.S. Magistrate Judge in West. Dist. of Washington
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of

Date and time issued: 11/05/2020 10:00 am


Judge's signature

City and state: Seattle, Washington

Hon. John L. Weinberg, United States Magistrate Judge
Printed name and title

Return

Case No.: MJ 20-713	Date and time warrant executed: 11/5/2020	Copy of warrant and inventory left with: N/A
-------------------------------	---	--

Inventory made in the presence of:

N/A

Inventory of the property taken and name of any person(s) seized:

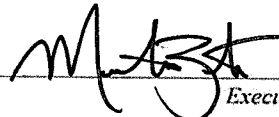
Information, including basic account holder/subscriber information, calendar info, account contacts, and email message content sent and received from the following email accounts:

- joshuasbusinessemail@gmail.com
- joshistopforever@gmail.com
- financingpsychology@gmail.com
- joshua.thomas.seattle@gmail.com
- proudtobeunamerican@gmail.com
- contactjoshuabales@gmail.com
- mastersshakejts@gmail.com
- summerofgeorge1@gmail.com
- joshuabcontact@gmail.com

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: **2/4/2021**


 Executing officer's signature
Matthew Zito Special Agent FBI
 Printed name and title

ATTACHMENT A

(Accounts to be Searched)

This warrant applies to information associated with the following email addresses (SUBJECT ACCOUNTS) that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway in Mountain View, California.

The SUBJECT ACCOUNTS, are:

joshuasbusinessemail@gmail.com

joshistopforever@gmail.com

financingpsychology@gmail.com

joshua.thomas.seattle@gmail.com

proudtobeunamerican@gmail.com

contactjoshuabales@gmail.com

mastersshakejb@gmail.com

summerofgeorge1@gmail.com

joshuabcontact@gmail.com

ATTACHMENT B**Particular Items to be Seized****I. Information to be disclosed by Google LLC (the "Provider")**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on November 2, 2020, the Provider is required to disclose the following information to the government for each SUBJECT ACCOUNT listed in Attachment A:

a. The contents of all emails associated with the account from January 1, 2018 to June 24, 2020, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken. The Provider is hereby ordered to disclose the above information to the government within 14 of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and instrumentalities of violations of Title 18, United States Code, Sections 2261A(2)(A), (B) (Cyberstalking); and Title 18, United States Code, Section 875(c) (Interstate Threats), those violations involving Joshua Bales and occurring after January 1, 2018, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Emails to and from the following email addresses:

a. [REDACTED]@gmail.com

b. [REDACTED]@uni.sydney.edu.au

(b) Photographs of X.C. or her personal items, such as underwear;

(c) Emails to X.C.'s family members, friends, and associates about X.C.;

(d) Emails about the sale or dissemination of information about X.C. or photographs of X.C.;

(e) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(f) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation; and

1 (g) The identity of the person(s) who created or used the email account, including records
2 that help reveal the whereabouts of such person(s).

3 This warrant authorizes a review of electronically stored information, communications, other
4 records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and
5 instrumentalities described in this warrant. The review of this electronic data may be conducted by
6 any government personnel assisting in the investigation, who may include, in addition to law
7 enforcement officers and agents, attorneys for the government, attorney support staff, and technical
8 experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic
9 data to the custody and control of attorneys for the government and their support staff for their
10 independent review.
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE
902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC, and my title is _____ . I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google LLC. The attached records consist of _____

[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)].

I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google LLC, and they were made by Google LLC as a regular practice; and

b. such records were generated by Google LLC's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature